State of Wisconsin
Department of Administration
Division of Enterprise Technology

SECURITY

Effective Date: 3/1/2018

System and Services Acquisition Standard

Purpose

The System and Services Acquisition standard provides documentation of the minimum requirements for IT Security considerations before and after the IT purchasing process to achieve compliance with the:

- Access Control Policy and Standard
- Configuration Management Policy and Standard
- Media Protection Policy and Standard
- Risk Management Policy and Standard
- Security Planning Policy and Standard
- System and Services Acquisition Policy

Standard

Ensure that DOA/DET IT acquisitions (equipment, software, and/or services) for DET/State IT systems and system environments, including those provided by third-party vendors, meet the security policies and standards required in the IT Security Policy Handbook and Standards (SA-9) and documented in DOA/DET procedures, as applicable.

Prior to IT Purchase/Acquisition

The listed items must be addressed and documented in the appropriate DET procedure/contract/service level agreement:

- Funding and resource allocation to incorporate appropriate information security requirements based upon the security plan (e.g. security requirements are included in the overall functional and nonfunctional requirements documentation) (PL-2, SA-2);
- Purchase and/or replacement of equipment, software, and/or services, occur throughout the System Development Life Cycle, SDLC (see the Risk Management Standard for detailed information about SDLC), therefore, the system purpose and high-level requirements should be documented in the requirements/justification for the purchase (SA-3);
- Procured equipment, software, and/or services must be done in compliance with applicable licensing agreements;
- Maintenance and support for information equipment, software, and/or services must be defined in the contract and/or service level agreement(s) (MA-6, SA-22);
- Disclosure of known vulnerabilities associated with the technology being acquired, and remediation (with testing) of said vulnerabilities prior to acceptance (SA-10, SA-11)

Effective Date: 3/1/2018

- The acquisition process must address the following explicitly or by reference in the contract (SA-4):
  - Security functional requirements needed to ensure security functions operate as intended (e.g. security capabilities, security functions, and security mechanisms)
  - Verification that security strength meets documented needs (e.g. associated with capabilities, functions, and mechanisms to include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass options)
  - Security assurance requirements to validate:
    - development processes, procedures, practices, and methodologies, and,
    - evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved;
  - Security-related documentation to provide user and administrator guidance regarding the implementation and operation of security controls;
  - Description of the information system environment(s) in which the system is intended to operate;
  - Acceptance criteria for information equipment, software, and/or services are defined in the same manner as such criteria for any organizational acquisition or procurement;
  - A requirement to restrict the location of equipment, software, and/or services that receive, process, store, or transmit DET/State information to areas within the United States territories, embassies, or military installations (SA-9).
- The following administrator and user documentation must be obtained upon purchase:
  - Documentation which states the security configurations for the technology (SA-4);
  - Documentation/guidance to set up secure configuration, installation and operation of the equipment, software, and/or services (SA-5);
  - Documentation for maintenance processes/procedures required for normal operation of the equipment, software, and/or services (SA-5); and,
  - Security features and functions accessible for use by the end-user (SA-5).

Post-procurement Requirements

The following are required for IT equipment, software, and/or services:

- IT System and Application Development Requirements
  - Development, configuration, set-up, maintenance, and removal must meet the requirements of the policies and standards listed above (SA-10, SA-11, SA-22);
  - Developers/installers of information system components must provide unique authenticators or change default authenticators prior to system use; and,
  - Developers/installers must verify that unencrypted static authenticators are not embedded in applications, access scripts, or stored on function keys (SC-8).

Effective Date: 3/1/2018

- DET must ensure that all equipment, software, and/or services are not allowed to fall out of their respective support timeframes.
- A description of the information equipment, software, and/or services and the environment in which the equipment, software, and/or services is intended to operate should be documented as determine in DET procedures (SA-4, SA-10, SA-11)

Definitions

- Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
- DET/State information - Any information that is created, accessed, used, stored, or transmitted by an Agency and/or DET.
- DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to: network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by DET.
- System Development Life Cycle, SDLC – A methodology used by an organization to effectively develop an information system. A typical SDLC includes five phases; initiation, development/acquisition, implementation/assessment, operations/maintenance, and disposal.

Compliance References

IRS Pub. 1075
NIST 800-53 Revision 4

Exception Process

Exceptions to this and all DET Security policies or procedures must follow the DET Exception Procedure.

Document History/Owner

This standard was developed as required by the Department of Administration, DET Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version	Approval/Revision/Review Date	Description	Approver/Author, Title
.1	6/24/2016	Original	Tanya Choice Cybersecurity Compliance Consultant

Effective Date: 3/1/2018

1.0		Final Approval	Bill Nash CISO

Authorized and Approved by:

Bill Nash	Bill Nash	3/1/2018
Print/Type	Signature	Date

Division of Enterprise Technology-Bureau of Security

Chief Information Security Officer